



Castilla-La Mancha

Píldoras Formativas de Ciberseguridad

Consejos para protegerse en verano

Julio 2026



En vacaciones bajamos la guardia, y precisamente eso es lo que buscan los ciberdelincuentes. Una actitud prudente suele ser la mejor herramienta de ciberseguridad.

Haz copias de seguridad de tus datos y configura la localización del dispositivo.

Los datos importantes almacenados en nuestros dispositivos pueden ser difíciles o imposibles de recuperar si el dispositivo se pierde o es robado.

Desactiva el bluetooth y el compartir archivos

El Bluetooth puede ser un punto de entrada para los ciberdelincuentes gracias a vulnerabilidades como *BlueBorne*. De igual manera, las funciones de compartir archivos pueden permitir el acceso no autorizado a tu dispositivo si no está protegido.

Activa la autenticación de dos factores (2FA)

Es una medida de seguridad esencial que añade una capa adicional de protección a tus cuentas en línea en lugar de depender únicamente de una contraseña.

No publiques que tu casa está vacía

Estás dando información útil tanto a ciberdelincuentes como a delincuentes comunes. Revisa la privacidad de tus publicaciones y comparte solo con familiares y amigos de confianza.



Actualiza tus dispositivos

Actualiza el sistema operativo del móvil, tablet y portátil. Actualiza las aplicaciones más utilizadas e instala los últimos parches de seguridad.

Evita usar redes Wi-Fi públicas

Especialmente para hacer pagos (como en cafeterías o aeropuertos), Los ciberdelincuentes pueden utilizar técnicas como el *sniffing* para capturar información transmitida a través de estas redes no seguras. Usa solo conexiones seguras o comparte la conexión desde tu móvil.

Cuidado con los correos electrónicos y mensajes sospechosos

En verano aumenta el número de fraudes sobre falsos envíos, reservas vacaciones, sorteos y ofertas. Utiliza tarjetas virtuales, PayPal u otras plataformas que protejan al comprador. Evita transferencias directas a vendedores desconocidos.

Bloquea siempre tus dispositivos

Nunca dejes móviles o portátiles desbloqueados en lugares públicos.

Utiliza:

- PIN robusto
- Huella dactilar
- Reconocimiento facial